EXTENSIONS OF REMARKS

INITIAL VICTORY IN THE STRUGGLE FOR FREEDOM OF THE PRESS IN RUSSIA—BUT THE FIGHT MUST GO ON

HON. TOM LANTOS

OF CALIFORNIA

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 27, 2000

Mr. LANTOS. Mr. Speaker, in the long and difficult fight for freedom of the press in Russia we have won an important victory today. The Russian prosecutor informed Vladimir Gusinsky—head of Russia's Media-Most media conglomerate—that the case against him has been dropped for ''the lack of a fact of a crime.''

Mr. Speaker, the prosecutor's action against Mr. Gusinsky was never simply a case of prosecuting a crime. From the beginning it has been a case of seeking to persecute and harass and intimidate and muzzle the free press in Russia. Vladimir Gusinsky is the head of Media-Most, which owns NTV television network, Russia's leading independent television network, as well as Echo of Moscow radio, and a number of other important independent media ventures.

It is significant, Mr. Speaker, that NTV and other Media-Most journalists have been critical of Russian President Putin and of the actions of the Russian government. Critical journalism is certainly nothing that would even raise eyebrows in the United States or Western Europe or other free countries around the world.

Mr. Speaker, the harassment of Mr. Gusinsky involved actions against him that go well beyond what would be done in a normal criminal proceeding involving such charges. Mr. Gusinsky was jailed for four days in June; in a high-handed fashion authorities seized documents from his company's offices several times; after he was released from jail, he was repeatedly called in for questioning; he was prohibited from traveling abroad; and steps were taken to freeze his personal assets.

On a number of occasions in the past, I have called to the attention of my colleagues in this House the systematic efforts to harass and intimidate the independent media in Russia. I hope that President Putin now understands that there is no room for Russia in the community of free and democratic nations if his government engages in efforts to oppress and threaten the free press in Russia.

Mr. Speaker, the dropping of charges against Mr. Gusinsky represents a victory for democracy and press freedom in Russia, but the battle is far from over. We must continue and strengthen our efforts to preserve free media in Russia.

INTRODUCTION OF THE FEDERAL INFORMATION POLICY ACT OF 2000

HON. THOMAS M. DAVIS

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 27, 2000

Mr. DAVIS of Virginia. Mr. Speaker, I rise today to introduce legislation that will endow the Federal Government with the ability to better coordinate and manage information technology policies governmentwide and transform the Federal Government into a national model for information resources management and information security practices. The Federal Information Policy Act [FIPA] of 2000 establishes an Office of Information Policy with a Chief Information Officer [CIO] for the United States and creates within that body, an Office of Information Security and Technical Protection [IN STEP]. This legislation harmonizes existing information resources management responsibilities now held by OMB and provides IN STEP with the responsibility for facilitating the development of a comprehensive, federal framework for devising and implementing effective, mandatory controls over government information security. In this latter respect, the Act is the logical complement to legislation I introduced in April, the Cyber Security Information Act of 2000, which seeks to encourage private sector information sharing with government in order to protect our national critical infrastructure. The Federal Information Policy Act will force the Federal Government to put its house in order and become a reliable public partner for protecting America's information highways.

For nearly four decades, information technology has been an integral component of information resources management [IRM] by the Federal Government. The Government's role as the single largest procurer of IT products and services in the 1960s and 1970s spurred the development of the U.S. computer industries that now form the backbone of our nation's New Economy. A decade ago, technology stood as one of many factors important to the mission and performance objectives of the Federal Government. Now both our economy and our society have become information-driven, such that IT plays the critical role in facilitating the Federal Government's ability to be effective and efficient in managing federal programs and spending, communicating with and providing services to citizens, and protecting America's critical infrastructure.

Five years ago, Congress recognized the crucial role played by technology when we called on the Administration to appoint a top-level officer to focus exclusively on the Year 2000 computer problem that threatened to undermine national commerce and government. This determination—that a single individual was needed to coordinate national and local cooperation to remediate computer systems and develop contingency plans—was based in part on an understanding of the interconnectivity of information systems within government, between government and the private sector, and within the private sector. The President heeded our recommendation and appointed John Koskinen to a Cabinet-level position as the chairman of the President's Council on Year 2000 Conversion.

Moreover, the Year 2000 computer problem highlighted two important deficiencies in the current Federal IRM structure. First, the Y2K scenario presented an important reminder that technology does not fill some amorphous role within the Federal Government. It is the ubiquitous thread that binds the operations of the Federal Government, and its efficient or inefficient use will make or break the ability of government to perform everything from the most mundane of governmental functions to the most critical national security measures. Second, the high degree of interdepence between information systems, both internally and externally, exposes the vulnerability of the Federal Government's computer networks to both benign and destructive disruptions. This factor is tremendously important to understanding how we devise a comprehensive and flexible strategy for coordinating, implementing and maintaining federal information security practices throughout the Federal Government as the rising threat of electronic terrorism emerges.

In following the lessons learned from the Y2K problem as well as the recent Love Bug viruses that affected many federal computer systems, the Federal Information Policy Act accomplishes four main purposes: (1) to revise chapter 35 of title 44 of the U.S. Code to establish a Federal Chief Information Officer to head the Office of Information Policy (OIP) within the Executive Office of the President; (2) to consolidate and centralize IRM powers currently allotted to the Office of Management and Budget [OMB] within the OIP; (3) to establish within the OIP the Office of Information Security and Technical Protection [IN STEP]; and (4) to establish a comprehensive framework implementing mandatory information security standards, and annual independent evaluations of agency practices in order to provide effective controls over Federal information resources. The Act creates a new chapter 36 to retain OMB's paperwork clearance functions that are currently contained in chapter 35 and are performed by the Office of Information and Regulatory Affairs.

This past May, at the Center for Innovative Technology in my congressional district, the House Government Reform Subcommittee on Government Management, Information, and Technology held a hearing in which we explored the strategies and challenges facing government in implementing electronic government initiatives. We learned that while electronic government initiatives promise to provide faster, more efficient, and convenient services, the Internet sets forth a wide array of challenges that must be addressed in order for the lower costs and improved customer service associated with electronic government to be realized. These include theft, fraud, consumer privacy protection, and the destruction